In re Application of: Yanovsky
Serial No.: 10/520,274
Filed: January 18, 2005
Office Action Mailing Date: April 22, 2008

Examiner: Shahrouz
Group Art Unit: 2132
Attorney Docket: 29238

REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1 - 48 are in this Application. Claims 1 – 48 have been rejected under 35 U.S.C. § 103. Claims 1, 21 and 37 have been amended herewith.

35 U.S.C. § 103 Rejections

Claims 1 – 48 have been rejected for lack of inventive step.

Claims 1, 21 and 37 have been amended to stress the point that the *encryption keys* are *generated separately* at the two different parties.

Seiheit does not teach that the encryption keys are generated separately at the two different parties. On the contrary Seiheit teaches a split key scheme in which part of the key is generated at one party and part of the key is generated at the other party. Subsequent to the generation of the two key parts a communication process takes place in which "this key component is then sent out on a communications channel from the transmitting user to the receiving user" Seiheit - abstract.

It is precisely this stage of transmission of the key or key part that the present invention was intended to avoid.

Likewise in Tan a single master key is generated at a single location. The master key is a long term master key which is used to generate subkeys for individual communications. As shown in the discussion in Tan column 9 the master key is generated by Alice from the pass phrase and never communicated to Bob. Thus the master key of Tan never fulfils the requirement of the claim that the encryption key is generated separately at the two different parties. The subkeys of Tan also never fulfil the requirement since the subkeys *are communicated* between the parties.

More particularly, US6,490,451 B1 by Daniel Tiong Hok Tan, teaches creating a data key for a message by using a long term secret master key and / or a seed, being held at both parties, or are generated by a secretly sent "pass phrase" (actually a key) in secure manner. Then, at message start, the sender generates a pseudo random couple of "start' and "length" data, or a triple of "start', "length" and "algorithm" and sends that to the receiver

unencrypted, to be used by both parties together with the secret long term master key for generating the working data key and the algorithm to be used.

In Tan, once an intruder discovers the secret master key, the whole system is exposed to him. Furthermore, there is a need to send in secure manner the master key, and / or the seed and / or the "pass phrase" each time.

The combination of Seiheit and Tan likewise fails to teach or suggest that the key is independently generated at the two parties, contrary to the requirement of claim 1.

An advantage of the present invention over either of Seiheit and Tan, is that the data that is shared between the parties can be sent over an open connection, say directly over the Internet. That is to say, there is a technical difference between exchanging keys and simply exchanging data, and the difference lies in whether or not an open link can be used. The present invention teaches for the first time the possibility of two parties separately generating keys from information that is not a key and can be shared over an open link.

The above comments apply to each of the independent claims 1, 21 and 37, which have each been amended to positively require that the key is separately generated at each party.

Claim 1 recites *inter alia*:

> "a key generator configured for separately generating at said first party a key for encryption/decryption based on said series of bits, thereby to *separately generate* a key at said first party which is *identical to a key likewise generated at said second party* based on said exchanged information,".

Claim 21 recites:

In re Application of: Yanovsky
Serial No.: 10/520,274
Filed: January 18, 2005
Office Action Mailing Date: April 22, 2008

Examiner: Shahrouz
Group Art Unit: 2132
Attorney Docket: 29238

"a key generator configured for *separately generating at each of said separate parties* cryptography keys".

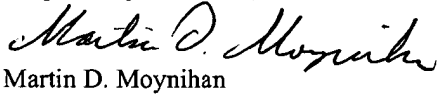
Finally claim 37 recites:

"using said derived data source to form cryptography keys *separately at different parties* at predetermined intervals."

The remaining claims are believed to be allowable as being dependent on an allowable main claim.

In view of the above amendments and remarks it is respectfully submitted that claims 1 - 48 are now in condition for allowance. A prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,



Martin D. Moynihan
Registration No. 40,338

Date: October 22, 2008

Enclosure:

- Petition for Extension (Three Months)